ISSN : 2301-7201

ITSMART

Vol 1. No 1. Juni 2012

Jurnal Teknologi & Informatika

Jurnal Ilmiah Teknologi dan Informasi

DAFTAR ISI

Pengaruh Variasi Panjang Kunci, Ukuran Blok, dan Mode Operasi Terhadap Waktu Eksekusi pada Algoritma Rijndael

Trihastuti Yuniati
Jurusan Informatika
Fakultas MIPA, UNS
Jl. Ir. Sutami 36 A Kentingan
Surakarta
three.sakha@gmail.com

Esti Suryani
Jurusan Informatika
Fakultas MIPA, UNS
Jl.Ir. Sutami 36 A Kentingan
Surakarta
suryapalapa@yahoo.com

Abdul Aziz
Jurusan Informatika
Fakultas MIPA, UNS
Jl. Ir. Sutami 36 A Kentingan
Surakarta
Abdul_7773@yahoo.com

ABSTRAK

Algoritma Rijndael merupakan salah satu algoritma kriptografi yang berjalan pada mode operasi cipher blok. Rijndael mendukung panjang kunci dan ukuran blok 128-bit sampai 256-bit dengan step 32 bit. Paper ini membahas bagaimana pengaruh variasi panjang kunci, ukuran blok dan mode operasi terhadap waktu eksekusi pada algoritma Rijndael. Eksperimen dilakukan terhadap empat berkas pdf berukuran berbeda, 2.5 MB, 5 MB, 10 MB, dan 20 MB. Keempat berkas tersebut dilakukan enkripsi dan dekripsi dengan berbagai kombinasi panjang kunci, ukuran blok, dan mode operasi. Variasi panjang kunci dan ukuran blok adalah 128-bit, 192-bit, dan 256-bit, dan variasi mode operasi adalah ECB, CBC, dan CFB. Tiap kombinasi diulang lima kali untuk mendapatkan waktu eksekusi rata-ratanya. Hasil penelitian menunjukkan bahwa kecepatan eksekusi pada mode ECB dan CBC sangat dipengaruhi oleh jumlah putaran, dimana jumlah putaran tergantung pada panjang kunci dan ukuran blok, sedangkan kecepatan eksekusi pada mode CFB relatif dipengaruhi oleh ukuran blok.

Keywords

algoritma Rijndael, cipher blok, kriptografi, mode operasi

1. PENDAHULUAN

Data merupakan salah satu aset yang sangat penting bagi siapapun, baik itu perusahaan, instansi pemerintahan, maupun institusi pendidikan. Data ini ada yang bersifat terbuka, artinya boleh diketahui oleh semua orang, dan ada yang bersifat rahasia, dimana hanya orang-orang tertentu yang boleh mengetahuinya. Data yang bersifat rahasia ini membutuhkan metode khusus untuk menjaga kerahasiaannya.

Berbagai upaya pengamanan data telah dilakukan untuk menjaga kerahasiaan data. Salah satu cara yang digunakan adalah dengan menyandikan data menjadi kode-kode yang tidak dimengerti. Penyandian dilakukan agar apabila data tersebut jatuh ke tangan pihak yang tidak berhak, pihak tersebut tetap tidak dapat memahami informasi yang sesungguhnya. Metode pengamanan data ini dikenal sebagai metode kriptografi. Berbagai macam algoritma kriptografi telah dikembangkan. Algoritma kriptografi yang baik akan memerlukan waktu yang lama untuk memecahkan data yang telah disandikan. Seiring dengan perkembangan teknologi komputer, dunia teknologi informasi membutuhkan algoritma kriptografi yang lebih kuat dan lebih aman, salah satunya adalah Rijndael. Algoritma ini memiliki keunggulan dalam hal performansi dan kesederhanaan kode, serta tingkat keamanan data yang tinggi untuk ukuran teknologi komputer yang ada saat ini [1], [2].

Sebagaimana algoritma blok cipher pada umumnya, algoritma Rijndael dapat dijalankan dalam beberapa mode operasi [3], [4]. Menurut [4] menunjukkan bahwa algoritma Rijndael dapat dijalankan dalam empat mode operasi, yaitu *Electronic Code Block* (ECB), *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB), dan *Output Feedback* (OFB), kunci 128-*bit*, 192-*bit*, dan 256-*bit*, dengan blok 128-*bit*. Menurut [5] dan [6] menunjukkan bahwa algoritma Rijndael mendukung variasi panjang kunci dan ukuran blok dari 128-*bit* sampai 256-*bit* dengan step 32-*bit*. Panjang kunci dan ukuran blok mempengaruhi jumlah putaran dalam proses enkripsi maupun dekripsi.

Analisa dilakukan terhadap algoritma Rijndael dengan ukuran blok 128-*bit* dan kunci 128-*bit*, 192-*bit*, dan 256-*bit* dijalankan dalam empat mode operasi (ECB, CBC, CFB, dan OFB) [3], sedangkan di dalam [6], analisa dilakukan terhadap algoritma Rijndael yang mendukung panjang kunci dan ukuran blok 128-*bit*, 192-*bit*, dan 256-*bit*, namun tidak ada variasi mode operasi. Kedua penelitian tersebut belum meneliti bagaimana pengaruh kombinasi dari variasi ketiga variabel (panjang kunci, ukuran blok, dan mode operasi) terhadap waktu eksekusi. Berangkat dari hal tersebut, maka dalam penelitian ini penulis bermaksud untuk menganalisa bagaimanakah pengaruh variasi panjang kunci, ukuran blok, dan mode operasi yang digunakan terhadap waktu eksekusi pada algoritma Rijndael.

2. LANDASAN TEORI

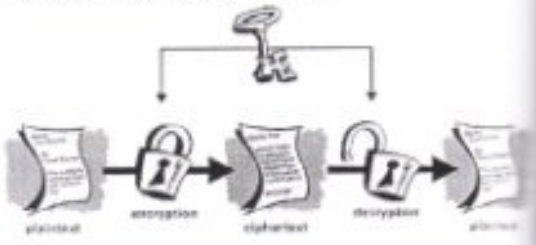
2.1 Kriptografi

Kriptografi secara umum adalah ilmu dan seni untuk menjaga keamanan pesan [7]. Sedangkan definisi kriptografi menurut [8], kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data.

Berdasarkan kunci yang dipakai, algoritma kriptografi dibagi menjadi dua [7], yaitu:

1. Algoritma kunci simetris

   Algoritma ini sering disebut sebagai algoritma klasik karena kunci yang digunakan untuk enkripsi sama dengan kunci untuk dekripsi. Keamanan dari pesan sangat tergantung pada kuncinya. Proses enkripsi-dekripsi dengan algoritma kunci simetris ditunjukkan oleh Gambar 1.



Gambar 1 Proses enkripsi-dekripsi dengan algoritma kunci simetris [15]